

	CRYPTOCURRENCY INVESTIGATIONS	Operations Order 7.34.00
	PHOENIX POLICE DEPARTMENT	NEW 11/25/24 PAGE 1

1. PURPOSE STATEMENT

To outline procedures for the initial response, investigation, and seizure of cryptocurrencies.

2. GENERAL DIRECTION

- A. To provide guidance on how to investigate and document crimes involving cryptocurrency, and information on cryptocurrency seizures. This Order does not address all aspects of digital currencies; for more information regarding cryptocurrency investigations contact the Property Crimes Bureau (PCB) Financial Crimes Detail, or refer to the [PCB manual](#).

3. DEFINITIONS:

A. Cold Storage Wallet	• A cryptocurrency wallet not connected to the internet. • Also known as Cold Storage or as a Cold Wallet. • The most common type of cold storage wallet is a Hardware Wallet (a small device that can be connected to a computer). • A Trezor is one common type of Hardware Wallet. * Trezors are similar in size to USB drives, but normally have a digital screen and input keys. • Other examples of cold storage wallets are Paper Wallets. * A Paper Wallet is when private and public keys are written on a piece of paper and stored for safekeeping.
B. Cryptocurrency	• Any form of digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of monies, operating independently of a central bank, including Bitcoin, Ethereum, Litecoin and Bitcoin Cash.
C. Cryptocurrency Wallet	• A location or account where cryptocurrency private and public keys are stored. Also called a Wallet.
D. Exchange	• A digital marketplace where traders can buy and sell cryptocurrencies using different fiat currencies or altcoins (crypto coins other than Bitcoin). • For example: a Bitcoin exchange is an online platform that acts as an intermediary between buyers and sellers of the cryptocurrency Bitcoin
E. Hot Storage Wallet	• A cryptocurrency wallet that is connected to the internet
F. Private Key	• A unique alphanumeric identifier that, together with a corresponding public key, allows access to cryptocurrency on the blockchain and is: * used to take ownership of cryptocurrency shared in a transaction. * intended to be kept secure and not shared, like a password or verification code. * a large number that can take many forms, such as a binary code, a hexadecimal code, or a QR code
G. Public Key	• A cryptographic code that allows a user to receive cryptocurrencies into their account or wallet, similar to bank account and routing numbers. • Public keys may be shared publicly; access to any associated cryptocurrency requires a private key.
H. Recovery Phrase (Seed Phrase)	• A group of 12 to 14 nonsensical words to gain access to your cryptocurrency wallet in the event the private key is lost, stolen, seized, or forgotten.
I. Virtual Currency	• Digital currency stored and transacted through designated software, mobile, or computer applications. • Transactions involving virtual currencies occur through secure, dedicated networks or the internet. • They are issued by private parties or groups of developers and are mostly unregulated.

	CRYPTOCURRENCY INVESTIGATIONS	Operations Order 7.34.00
	PHOENIX POLICE DEPARTMENT	NEW 11/25/24 PAGE 2

4. **PROCEDURES**

A. **Initial Response:**

- (1) Cryptocurrency transactions are irreversible. Do not seize, shut down, or attempt to remove funds from inside a cryptocurrency ATM.
- (2) For in progress calls be aware the victim could be on the phone with the suspect upon your arrival and could be reluctant to provide information.
- (3) Be aware that papers or receipts containing bitcoin addresses, private and public keys, seed phrases, and cold wallet storage devices may be in plain view.
- (4) When completing the original report include as much detail as possible listing the type of cryptocurrency, complete transaction information such as location, date, time, transaction hash, receiving address, quantity of crypto purchased, value of crypto purchased, etc.
- (5) Collect and photograph any Bitcoin ATM transaction receipts, cryptocurrency addresses, or QR Codes.
- (6) If the victim removed funds from a bank account document the date, time, location, bank name, account number and withdrawal amount.
- (7) Photograph and collect any bank receipts.
- (8) If the victim had their own cryptocurrency account at an exchange, document the exchange, account number, transaction history to include all relevant transaction ID's and cryptocurrency addresses.
- (9) Document any phone numbers, email addresses, or websites used in the completion of the crime.
- (10) Advise the victim to file a complaint with the cryptocurrency ATM business (ie. Bitcoin Depot, Athena Bitcoin). Some cryptocurrency ATM businesses will reimburse transaction fees for fraudulent transactions if requested within a few days of the initial transaction. Cryptocurrency ATM fees are significant and can account for approximately 30 percent of the entire transaction.
- (11) Instruct the victim to also file a complaint with the FBI Internet Crime Complaint Center at www.IC3.Gov.

B. **Notifying the Financial Crimes Detail**

- (1) Cryptocurrency transactions move rapidly. The Financial Crimes Detail can trace cryptocurrency transactions.
- (2) For any cryptocurrency transaction occurring within the last 24 hours:
 - (a) During normal business hours (M-F 0600-1600) contact the Financial Crimes Detail Sergeant at 602-896-7831.
 - (b) After hours contact the on-call Property Crimes Bureau Sergeant through the VCB Desk Sergeant at 602-262-6147.
- (3) For any cryptocurrency transactions occurring more than 24 hours ago:
 - (a) Email the Financial Crimes Detail at documentcrimes@phoenix.gov

	CRYPTOCURRENCY INVESTIGATIONS	Operations Order 7.34.00
	PHOENIX POLICE DEPARTMENT	NEW 11/25/24 PAGE 3

4. B. (3) (b) Include the report number, victim name and telephone number, photos of cryptocurrency transaction receipts to include the transaction hash, receiving address, and QR code.

C. **SEIZURE OF CRYPTOCURRENCY**

- (1) Digital Currency can be subject to seizure either as evidence, by forfeiture, or both.
- (2) Seizures of cryptocurrency will only be completed with the approval, and under the direct supervision, of the Financial Crimes Detail Sergeant.
- (3) The procedures used by the Financial Crimes Detail to seize cryptocurrency can be found in the Property Crimes Bureau Manual.

Last Organizational Review: